EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Dawn-Marie Bey on 7/15/08.

The Attorney of record, Dawn-Marie Bey, gave the Examiner authorization to cancel claims 51-53. Claims 51-53 are now cancelled.

Reasons for Allowance

2. Claims 34-50 are allowable for the following features, "generating binary vectors representing the presence and absence of port-specific activities based on each packet with each port module; assessing each binary vector and determining a level of expertise and deception for the port-specific activities represented by the binary vector with each port module; and outputting a behavioral rating from each port module in real-time based on the assessing and determining steps, the behavioral rating includes at least two dimensions of deception and expertise", as example of prior art that does not disclose this is Botros. Botros discloses user activity files and historical data are used as input to a feature generator or builder. The feature generator is implemented involving an equation for calculating a time-weighted mean. The output from feature generator is a features list. The features list contains features which can be classified into several different categories. Individual features from features list are used as input

to a model. Botros does not look at packets in real-time, Botros discloses historical data and logs of past activity which are analyzed for threats. Botros discloses a system for training a neural network using historical data from users. Botros discloses samples of current activity on a specific network to differentiate between intrusive behavior and regular network activity. In contrast, the Applicant discloses a system whereby behaviors are rated based upon the presence of expertise and deception and a neural network is trained to return a rating for expertise and deception for any combination of human behaviors.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

July 15, 2008
/J. E. J./
Examiner, Art Unit 2139

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139